US needs to be prepared for Russian cyber-retaliation

Frank J. Cilluffo and Sharon L. Cardash, GWU Homeland Security Policy Institute

The latest chapter in the conflict over Ukraine involves the imposition of sanctions by the United States and the European Union against Sberbank, and against Rosneft, the heavyweight among Russia's state-owned oil companies. While it has taken some time for this particular shoe to drop, the consequences could be significant.

blackred | Getty Images

Taken in tandem with previous sanctions, all the energy "bigs" in Russia are now in the crosshairs, along with the major banks that were already part of a previous round of targeted sanctions initiated in response to continued Russian moves against Ukraine. While Sberbank and Gazprom may not be household terms in the West, they are giants in Russia. Keep in mind that energy and banking are among the most critical of critical infrastructures, so hitting them with sanctions is hitting where it truly hurts. Despite buoyant Russian rhetoric, the impending reality for Russia's energy and banking sectors is unlikely to be so rosy.

Every action has a reaction, however, and Russia's response to the West's latest step remains to be seen. What we do know, though, is that Russia has long integrated cyber operations into its larger military strategy and doctrine. Indeed, Russia's campaign against Ukraine has invoked such strategy and tactics, using cyberattacks to disrupt Ukraine's communications systems, and information warfare to engage in psychological battle against the Ukrainian government and broader publics. These attempts to undermine Ukrainian authorities and deny them maneuverability also aimed to foster and maintain a spirit of resistance to Kiev among pro-Russian forces within Ukraine.

Against this background, it is no great leap to suggest that Russia may consider turning its cyber skills against those who initiated sanctions on Russian behavior, just as the heat in the kitchen rises. From a Russian perspective, this would fall into the category of turnabout is fair play. Cyberattacks have the added attraction of plausible deniability, since it is

difficult to trace with full certainty the source of an attack. Russia can also place itself at a further level of remove by relying upon proxies for their cyber operations as they have in the past. With the latest round of sanctions as a potential spur to Russian escalation along these lines, U.S. energy and banking executives in particular — not just chief information security officers and chief security officers—should take the threat seriously, with CISOs and CSOs being on the lookout for indicators.

In short, the cyber domain is the new battlefield, and U.S. energy and banking concerns are on the front lines, with a responsibility to shareholders to take necessary and appropriate steps to protect the firm — in partnership with government, to the extent that it is both willing and able. In fact, we may have seen the "turnabout is fair play" adage in practice already, with the recent cyber incident involving JPMorgan Chase in which hackers breached the bank's servers. While the full nature of the compromise in that case is still being investigated, its sophistication and planning suggests the possible involvement of a foreign government. Consider also that at least three other U.S. banks have been targeted — and the U.S. events may be connected to recent cyberattacks on European banks.

Moving forward, it will be crucial to do all that we can to deny Russia (or any adversary) the opportunity to wreak cyber-havoc with U.S. critical infrastructure such as the finance and banking sector. After all, it only makes sense to throw the first punch if we have the capacity to withstand and prevail if a powerful swing comes back in our direction. Making clear to Russia that deplorable actions have consequences was, and remains, the right thing to do. But we need to do more, urgently, to inoculate ourselves.

One important step in that direction would be for Congress to pass legislation soonest in order to facilitate and support information sharing between and among entities in the public and private sectors, to help meet and defeat the cyber threat—which encompasses, but is by no means limited to, possible Russian cyber-retaliation. To this end, there is no shortage of ideas or bills on the table. These include initiatives spearheaded by Senators Dianne Feinstein and Saxby Chambliss (jointly); Senator Kirsten Gillibrand's proposal for tax credits to incent information sharing; and Representative Michael McCaul's bill to enhance the role of the Department of Homeland Security's National Cybersecurity and Communications Integration Center. While no single proposed measure may be perfect in the eyes of all, we must not let perfection become the enemy of the good. Any of the proposed actions cited would assuredly be better than none at all.

Russian President Vladimir Putin has demonstrated time and again that he is willing to push Western boundaries, both literally and figuratively. The time for all of us to counterpunch back on that front is now.

Commentary by Frank J. Cilluffo and Sharon L. Cardash. Cilluffo served as special assistant to the president for Homeland Security, and is now director of the George Washington University Cybersecurity Initiative, and GW's Homeland Security Policy Institute. Cardash is HSPI's associate director, and a founding member of GW's Cyber Center for National & Economic Security. Follow the Homeland Security Policy Institute on Twitter @HSPI.